

Week 3- Securing Cloud Storage

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

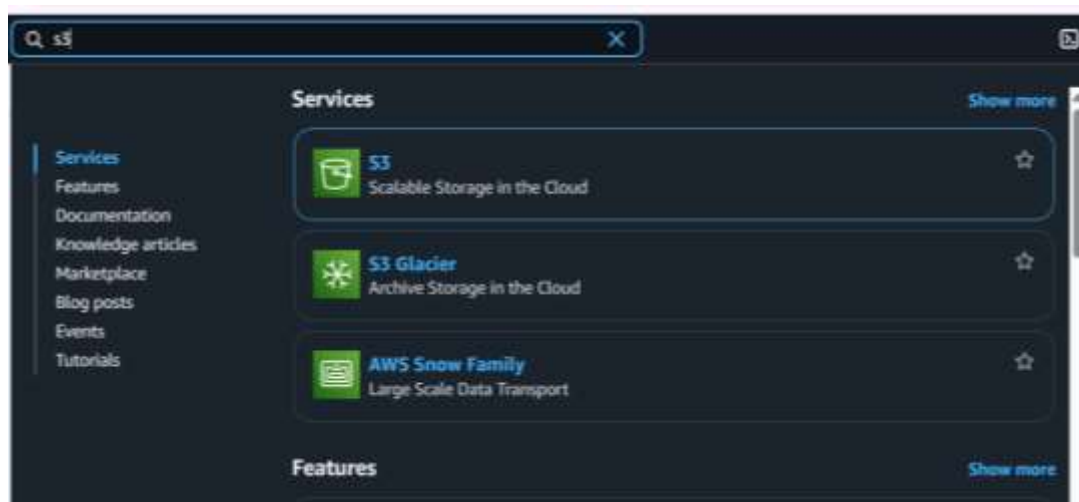
Email Id- samruddhi.nikam_24ucs@sanjivani.edu.in

College Name- Sanjivani University

- ❖ **Task-** 1) Set up S3 bucket .
2) Apply access control policies.
3) Document security configurations.

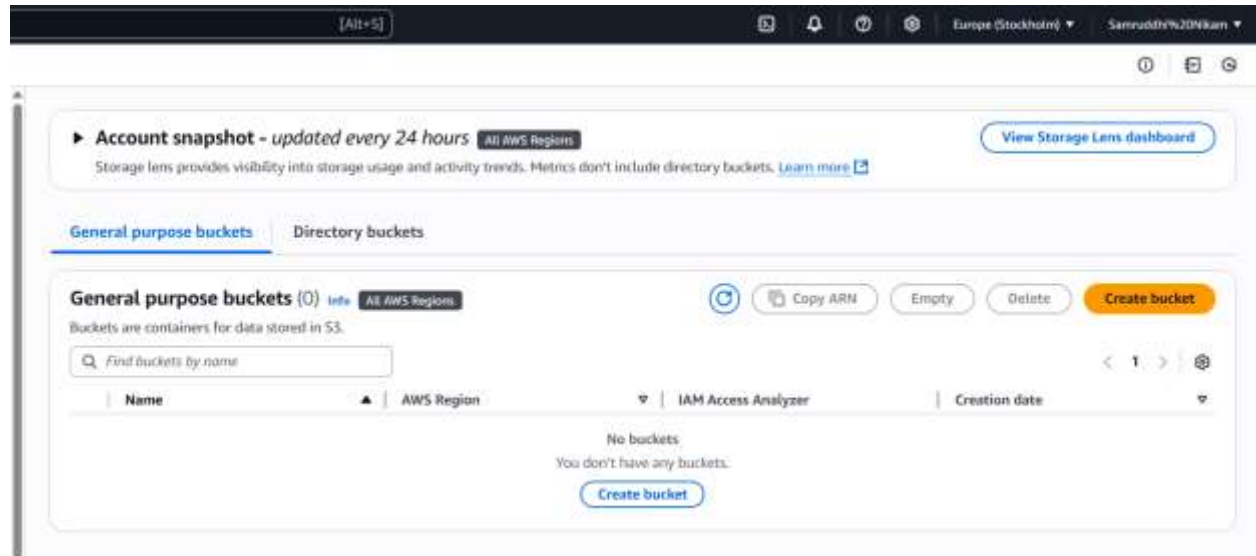
🚦 Step Set up S3 Bucket.

1. Logged in to AWS Console.
2. Search S3 and then click.

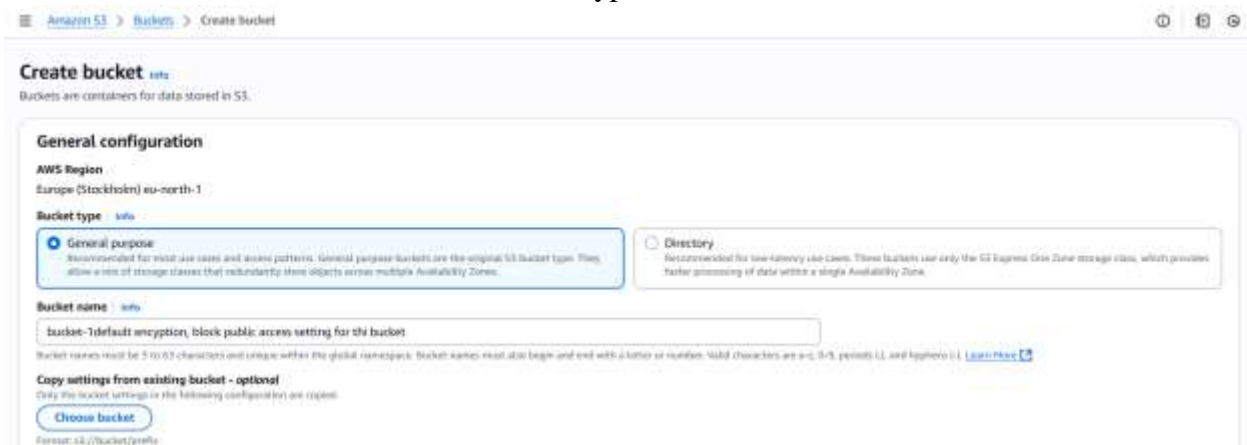


3. Then Click Create bucket Option.

Week 3- Securing Cloud Storage



4. Enter the Bucket name and select the Bucket type.



5. Select the Object Ownership



Week 3- Securing Cloud Storage

6. Block Public access Setting for this bucket.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- ☐ **Block public access to buckets and objects granted through new access control lists (ACLs)**
It will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting does not change any existing permissions that allow public access to S3 resources using ACLs.
- ☐ **Block public access to buckets and objects granted through any access control lists (ACLs)**
It will prevent all ACLs that grant public access to buckets and objects.
- ☐ **Block public access to buckets and objects granted through new public bucket or access point policies**
It will block new bucket and access point policies that grant public access to buckets and objects. This setting does not change any existing policies that allow public access to S3 resources.
- ☐ **Block public and cross-account access to buckets and objects through any public bucket or access point policies**
It will prevent all policies that grant public access to buckets and objects.

7. Select Bucket versioning Enable, and then select Default encryption server-side encryption with amazon S3managed keys(SSE-S3).

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. You can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

☐ Disable

☒ Enable

Tags - optional (0)

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

- ☒ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☐ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

8. Select Bucket key Enable, and then click create bucket button.

☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)

Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by eliminating calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

☐ Disable

☒ Enable

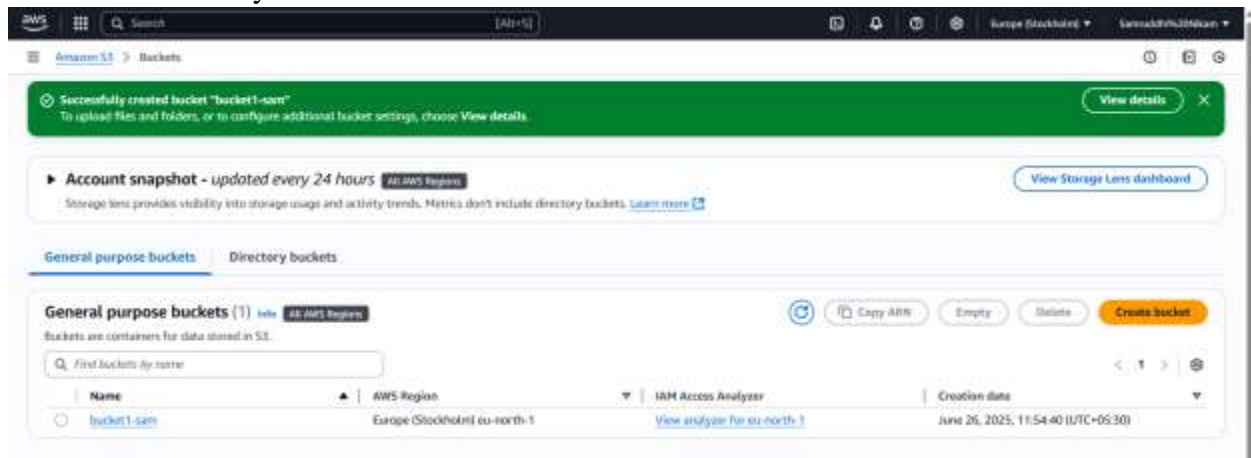
Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

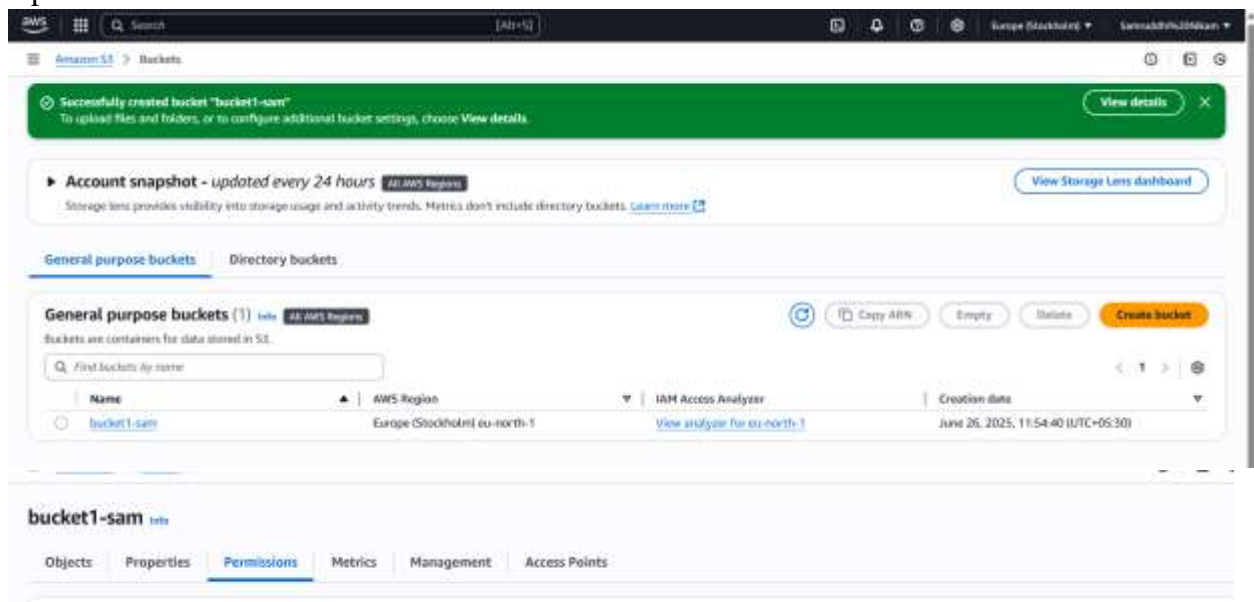
Week 3- Securing Cloud Storage

9. Bucket Successfully Created.



+ Steps Apply Access control Policies.

1. Open S3 > Bucket > bucket1-sam > Permission.



2. Scroll- down and Click Edit.

Week 3- Securing Cloud Storage

Bucket policy

EditDelete

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket

To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#)

No policy to display.

Copy

3. Then Write then write the following code to block public access, and save the policy.

Policy

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "AllowOnlyOwner",
6       "Effect": "Deny",
7       "Principal": "*",
8       "Action": "s3:GetObject",
9       "Resource": "arn:aws:s3:::bucket1-sam/*",
10      "Condition": {
11        "StringNotEquals": {
12          "aws:PrincipalAccount": "355433852359"
13        }
14      }
15    }
16  ]
17 }
18
```

4. Save the policy → Now only the bucket owner's account can access the objects. All other access is denied.

Week 3- Securing Cloud Storage

The screenshot displays the Amazon S3 console interface for a bucket named 'bucket1-sam'. At the top, a green notification bar states 'Successfully edited bucket policy.' Below this, a section titled 'Individual Block Public Access settings for this bucket' is visible. The main section is 'Bucket policy', which includes a warning: 'Public access is blocked because Block Public Access settings are turned on for this bucket.' It also provides a JSON policy snippet and a 'Copy' button. Below the bucket policy, another green notification bar says 'Successfully edited bucket policy.' The 'Access control list (ACL)' section follows, with a warning about the bucket owner enforced setting. A table lists the grants for the bucket, including the bucket owner, everyone (public access), authenticated users group, and S3 log delivery group.

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket. To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3::bucket1-sam/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "555453852359"
        }
      }
    }
  ]
}
```

Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

This bucket has the bucket owner enforced setting applied for Object Ownership. When [bucket owner enforced](#) is applied, use bucket policies to control access. [Learn more](#)

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID: 7e5611fed77b0afac3fa4039110b2846dda78bd3cd0ff1a6dc70bd3c3c02427f	List, Write	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group: http://acs.amazonaws.com/groups/s3/LogDelivery	-	-

Task 3- Document security configurations.

- Default encryption with Amazon S3 managed keys (SSE-S3) is enabled to protect all objects by default.

The screenshot shows the 'Default encryption' settings for a bucket. It indicates that server-side encryption is automatically applied to new objects. The encryption type is set to 'Server-side encryption with Amazon S3 managed keys (SSE-S3)'. The bucket key is also set to 'Enabled'.

Default encryption [info](#) [Edit](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [info](#)
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

Week 3- Securing Cloud Storage

- Versioning is enabled to keep all versions of objects for recovery and rollback

Edit Bucket Versioning [info](#)

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
☐ Suspend
This suspends the creation of object versions for all operations but preserves any existing object versions.
☒ **Enable**

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)
Disabled

- Access policy restricts object access to only the bucket owner's account

Bucket policy [Edit](#) [Delete](#)
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowOnlyOwner",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::bucket1-sam/*",
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": "355433852359"
        }
      }
    }
  ]
}
```

[Copy](#)

- Public access is blocked using AWS's Block Public Access settings for added security.

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#)